10.00 Equipment Management ***Effective Date: 7/28/08***
10.03 System Security

PURPOSE: To detail processes local agencies must follow to protect client confidentiality and to prevent unauthorized access to WIC data.

A. POLICY

1. Computers and telecommunication resources (the Internet) purchased with WIC funds may be used for business purposes only.

2. Local agencies shall maintain security measures to safeguard all WIC equipment.

3. Physical Security

   a. Stationary computers shall be equipped, when reasonable, with devices that secure hardware.
   b. Portable equipment shall be under the supervision of staff and shall not be left unattended.
   c. If portable equipment is used by multiple staff, the local agency shall maintain a log of users and dates equipment is taken and returned.
   d. Local agencies shall maintain current anti-virus software on all WIC computers used for MI-WIC.
   e. All computer workstations must be positioned or located in a manner that will minimize the exposure of any displayed client data.
   f. Local agency staff must comply with state and federal laws and regulations regarding the proper acquisition, use and copying of copyrighted software and commercial software licenses.

4. System Access

   a. Each user will have his/her own distinctive Single Sign On account.
   b. The WIC Coordinator shall be responsible for maintenance of all clinic user access to the MI-WIC system within the local agency.
   c. The WIC Coordinator shall assign role permissions to users based on their responsibilities in the clinic, and WIC policy requirements.
   d. At the time of termination from a local WIC agency clinic, or a reassignment to another non-WIC program, all user roles must be removed from MI-WIC for that employee.

5. Local Agency User Requirements

   a. All local agency staff shall have access to the Internet and MI-WIC.

b. All users must sign and abide by the terms of a MI-WIC User Security and Confidentiality Agreement (See 10.04A MI-WIC User Security and Confidentiality Agreement).
c. User ID's and passwords shall not be shared with other individuals.
d. User ID's and passwords must not be documented, written or otherwise stored in an unsecured manner.

6. MI-WIC User Security and Confidentiality Agreements shall be kept current as long as the agency staff member has access to MI-WIC confidential information. The Agreement shall be updated if the employee's role changes within the WIC program. The Agreements shall be retained by the local agency for three years 150 days beyond employment by the local agency.

References:
45 CFR 164.310
State of Michigan Computer Crime Law (Public Acts 1979-No.53)

Cross-references:
1.03 Confidentiality
10.04 MI-WIC Access